Analisis Penambahan metode Naive Bayes Sebagai Klasifikasi Serangan pada Web Server dengan IDS Snort

RASYID MAULID MAJID
(Pembimbing : Elkaf Rahmawan P., M.Kom)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201307417@mhs.dinus.ac.id

ABSTRAK

Di zaman modern ini mengakses informasi lebih mudah dengan adanya internet, tetapi dengan kemudahan ini ada beberapa orang yang menanfaatkannya untuk tujuan tidak baik seperti mencuri data yang penting dan sensitif hingga perusakan system. Oleh karena itu keamanan data merupakan prioritas yang penting bagi pengguna sistem. Ada beberapa penelitian untuk menambah keamanan system seperti menggunakan metode Naive Bayes Klasifikasi dan IDS Snort yang memiliki kelebihan dan kekurangan masing-masing. Meskipun begitu serangan yang dilakukan untuk mencuri data dan pengrusakan sistem akan terus berkembang dengan seiringnya waktu sehingga menjadi lebih sulit untuk dideteksi. Tujuan dari penelitian ini adalah memberikan alternatif keamanan yang lebih baik untuk mendeteksi serangan pada web server. Penelitian ini akan menganalisis peningkatan deteksi serangan pada traffic serangan dengan dua metode, seperti filtering traffic serangan dengan Tools Snort dan klasifikasi serangan dengan Metode Naive Bayes pada traffic serangan. Hasil dari penelitian dengan dua metode Tools Snort mampu mengidentifikasi sebanyak 6 paket serangan dan klasifikasi serangan sebanyak 2964 paket serangan. Dari Hasil penelitan tersebut, hal ini dapat disimpulkan bahwa identifikasi serangan yang dilakukan oleh Naive Bayes mengalami peningkatan.

Kata Kunci : Klasifikasi Naive Bayes, Snort, Honeypot, Web Server

Analysis Of Naive Bayes Method Addition For Classification Of Attack On Web Server By IDS Snort

RASYID MAULID MAJID
(Lecturer : Elkaf Rahmawan P., M.Kom)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201307417@mhs.dinus.ac.id

ABSTRACT

In this modern era, accessing information becomes easier by using the internet, but there are some people who use it for unkind purposes such as stealing important and sensitive data until the destruction of the system. Because of that, securityâ€™s data is an important priority for a user. There are several studies to add securityâ€™s system such as using the Naive Bayes Classification and Snort IDS methods which have their advantages and disadvantages. Nevertheless, the attacks which carried out to steal data and destruction of the system will continue to evolve with time so it becomes more difficult to detect. The purpose of this research is giving a better security alternative to detect the attacking the web server. This research will analyze the increase of attack detection on trafficâ€™s attack by two methods, such as filtering attack traffic with Snort Tools and attack classification with Naive Bayes Method on attack traffic. The results of the study by two methods of Snort Tools are able to identify as many as 6 attack packets and the attack classification with a total of 2964 attack packets. From the results of this research, it can be concluded that the identification of attacks conducted by Naive Bayes has increased.

Keyword : NaÃ¯ve Bayes classification, Snort, Honeypot,Web Server